Модель угроз безопасности информации при её обработке в информационной системы персональных данных ГАПОУ«Педколледж» г. Орска

г. Орск 2020

1. Обозначения и сокращения

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

НДВ – недекларированные возможности

НСД – несанкционированный доступ

ОБПДн – обеспечение безопасности персональных данных

ПДн – персональные данные

ПО – программное обеспечение

СВТ – средство вычислительной техники

СЗИ – средство защиты информации

ТКУИ – технический канал утечки информации

УБПДн – угрозы безопасности персональных данных

2. Термины и определения

В настоящем документе используются следующие термины и их определения:

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может

быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество,

дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3. Нормативные ссылки

При формировании настоящей Модели угроз безопасности информации использовались следующие нормативно-правовые документы:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 года;

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 года;

– Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru);

4. Общие положения

Информационная система персональных данных «Модель угроз безопасности информации при её обработке в информационной системы персональных данных ГАПОУ «Педколледж» г. Орска» (далее – ИСДн) предназначена для формирования, обработки, хранения и предоставления данных о работе в рамках отношений, указанных в Федеральном законе от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Решение о создании ИСПДн принято на основании _____ от __.__.20__ № _____ «……».

В соответствии с актом классификации ИСПДн от __.__.20__ № __ утверждённым ___ и по результатам анализа исходных данных ИСПДн имеет 4 уровень защищенности персональных данных (УЗ 4).

В ИСПДн могут обрабатываться следующие персональные данные:

фамилия, имя, отчество;
место, год, дата рождения;
адрес проживания;
адрес электронной почты;
сведения об образовании;
сведения о трудовой деятельности;
сведения о трудовом стаже;
телефонный номер;
семейное положение;
данные о наградах, медалях, поощрениях, почетных званиях;

В соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», оператор ИСПДн при обработке персональных данных (далее - ПДн) обязан принимать правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя определение угроз безопасности ПДн при их обработке и формирование Модели угроз.

Модель угроз содержит данные по угрозам, связанным с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, неправомерного распространения информации или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них информации с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования защищаемой информации.

В Модели угроз представлена оценка исходного уровня защищенности защищаемой информации, а также анализ угроз безопасности информации.

Анализ угроз безопасности информации включает:

описание угроз;

оценку вероятности возникновения угроз;

оценку реализуемости угроз;

оценку опасности угроз;

определение актуальности угроз.

К информационным ресурсам ИСПДн осуществляется удаленный доступ сотрудников других организаций по незащищенному каналу связи.

Модель угроз может быть пересмотрена:

– по решению владельца ИСПДн на основе периодически проводимых им анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений данной ИСПДн;

– в случае модернизации ИСПДн;

– в случае изменения масштаба ИСПДн или значимости обрабатываемой в ней информации;

– по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности защищаемой информации при её обработке в ИСПДн;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности информации;

– в случае обнаружения новых угроз внесенных в банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru);

– изменения требований законодательства Российской Федерации в области защиты информации, нормативно-правовых актов и методических документов, регулирующих защиту информации.

5. Описание информационной системы и особенностей её функционирования

ИСПДн включает в себя совокупность содержащейся в базе данных информации и обеспечивающих ее обработку с помощью информационных технологий и технических средств, соответствующих действующему законодательству.

ИСПДн обеспечивает формирование, автоматизированную обработку, хранение и предоставление данных о деятельности ГАПОУ «Педколледж».

ИСПДн содержит:

информацию о деятельности ИСПДн;

инструкции по работе с ИСПДн;

информацию о планируемых перерывах в работе ИСПДн;

иную информацию, размещение которой не противоречит законодательству Российской Федерации.

Параметры ИСПДн, содержащие ПДн, определяющие уровень защищенности ПДн приведены в таблице 1.

Таблица 1

Подключение ИС к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим разграничения прав доступа пользователей	Не имеется
Категория ПДн, обрабатываемых в ИС	Общедоступные
Категории субъектов ПДн, обрабатываемых в ИС	Субъекты, не являются сотрудниками
Объем ПДн, обрабатываемых в ИС	Менее 100 000 субъектов
Тип угроз	Угрозы 3-го типа
Уровень защищенности ПДн, обрабатываемых в ИСПДн	4
Заданные характеристики безопасности ПДн	Целостность, доступность

В соответствии с актом классификации от 18.09.2020 и исходя из вышеуказанных характеристик, в ИСПДн установлен 4 уровень защищенности ПДн (УЗ4).

Определение уровня исходной защищенности ИСПДн.

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Уровень исходной защищенности ИСПДн определен экспертным методом в соответствии с «Методикой определения актуальных угроз

безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Методика), утвержденной 14.02.2008 г. заместителем директора ФСТЭК России.

Для определения уровня исходной защищенности производится оценка этих характеристик по трем качественным показателям: «Высокий», «Средний» и «Низкий».

В соответствии с Методикой уровень защищенности определяется следующим образом:

1. ИСДПн имеет «Высокий» уровень исходной защищенности, если не менее 70% характеристик ИС соответствуют уровню «Высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – уровню «Средний»;

2. ИСПДн имеет «Средний» уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «Средний», а остальные – «Низкому» уровню;

3. ИСПДн имеет «Низкий» уровень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

1.1.1. При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент(Y_1), а именно:

высокий – Y_1= 0;

средний – Y_1= 5;

низкий – Y_1= 10.

1.1.2. Технические и эксплуатационные характеристики ИСПДн, определяющие уровень исходной защищенности ИСПДн, приведены в таблице 2.

Таблица 2

Характеристика	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. Территориальное размещение			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	-	-	+
2. Наличие соединения с сетями общего пользования			
ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. Встроенные (легальные) операции с записями баз данных			
чтение, поиск;	+	-	-

4. Разграничение доступа к данным			
ИСПДн с открытым доступом	-	-	+
5. Наличие соединений с базами данных иных ИС			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	-	-
6. Уровень обобщения (обезличивания) ПДн			
ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	-	-	+
7. Объем данных, которые предоставляются сторонним пользователям ИС без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с ПДн;	-	-	+

1.2. Соотношение характеристик ИС, соответствующих разным уровням защищенности, определенные на основании данных таблицы 3:

- 28.5% характеристик ИС соответствуют *высокому* уровню защищенности;
- 14.3% характеристик ИС соответствуют *среднему* уровню защищенности;
- 57.2% характеристик ИС соответствуют *низкому* уровню защищенности.

1.3. Уровень исходной защищенности ИС: ***низкий***. Таким образом, коэффициент исходной защищенности $\mathbf{Y_1 = 10}$.

1.4. Взаимодействие ИСПДн с другими информационными системами не предполагается.

6. Возможности нарушителей (модель нарушителя)

Модель нарушителя представляет собой абстрактное описание нарушителей информационной безопасности как источников угроз безопасности, а также предположения об их возможностях, которые могут быть использованы для разработки и проведения атак, и ограничениях на эти возможности.

Целью построения Модели нарушителя является определение типа возможного нарушителя безопасности персональных данных при их обработке в ИСПДн.

В качестве объектов атак рассматриваются защищаемая информация, сопутствующая информация, программное обеспечение ИСПДн, технические средства ИСПДн, помещение, в котором расположены технические средства.

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы расположенных в контролируемой зоне (далее – КЗ) нарушители подразделяются на два типа:

внешние нарушители (тип I) – лица, не имеющие права физического доступа к техническим средствам информационной системы, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к техническим средствам информационной системы, ее отдельным компонентам.

Границы КЗ ИСПДн определяются Приказом «О персональных данных» от 18.09.2020 № ___.

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

несанкционированный доступ (далее – НСД) может быть следствием как случайных, так и преднамеренных действий;

нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;

проведение работ по разработке, созданию способов и средств атак в организациях, специализирующихся в области разработки и анализа ПО, СЗИ и СКЗИ, не является целесообразным для нарушителей с учетом высокой стоимости разработки и создания способов и средств атак, который в итоге может нанести незначительные негативные последствия как для ИСПДн и содержащейся в ней информации, так и для субъектов ПДн.

В таблице 3 представлены потенциальные нарушители ИСПДн.

Таблица 3

Субъект	Тип нарушителя		Возможные цели (мотива угроз безопасности
	Внешний (I)	Внутренний (II)	
Специальные службы иностранных государств	+	-	Дискредитация или деятельности органа власти субъекта РФ
Преступные (хакерские) группы	+	-	Причинение имущественно мошенничества или и путем. Выявление уязв их дальнейшей прода финансовой выгоды
Физическое лицо, не являющееся служащим ГАПОУ «Педколледж» г. Орска	+	-	Идеологические или поли Причинение имущест путем мошенничест преступным путем. Ж желание самореализаци статуса). Выявление уязвимостей дальнейшей продажи финансовой выгоды
Разработчики ИСПДн и программного обеспечения (обеспечивающие техническую поддержку)	+	-	Внедрение дополнительных возможностей в обеспечение или технические средст разработки. Причинение имущественно обмана или злоупотребл Непреднамеренные, неос неквалифицированные д
Лица, имеющие санкционированный доступ к серверам на которых размещена ИСПДн, но не имеющие доступа к информации (обслуживающий персонал (охрана, работники административно-хозяйственных служб))	-	+	Причинение имущественно обмана или злоупотре Непреднамеренные, не неквалифицированные д

Администратор ИСПДн	-	+	Причинение имущественно мошенничества или и путем. Любопытство самореализации (подтве Месть за ранее соверш Выявление уязвимост дальнейшей продажи финансовой выгоды. Н неосторожные или нек действия
Администратор безопасности	-	+	Причинение имущественно мошенничества или и путем. Месть за ранее совершенны Выявление уязвимостей дальнейшей продажи финансовой выгоды. Н неосторожные или нек действия
Бывшие работники (пользователи)	+	-	Причинение имущественно мошенничества или и путем. Месть за ранее совершенны

В качестве нарушителей информационной безопасности ИСПДн имеет смысл рассматривать исключительно субъектов, перечисленных выше, действующих либо самостоятельно, либо вступивших в сговор между собой. Модель нарушителя информационной безопасности ИСПДн строится исходя из конкретных категорий субъектов, их квалификации, потенциала и мотивации действий.

Возможности каждого нарушителя (субъекта) по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в ИСПДн.

В зависимости от потенциала, требуемого для реализации угроз безопасности защищаемой информации, обрабатываемой в ИСПДн, нарушители подразделяются на:

нарушителя, обладающим базовым (низким) потенциалом - возможности уровня одного человека, подразумевается, что для реализации атак могут использовать информацию только из общедоступных источников, а также могут приобретать и использовать специальные средства эксплуатации уязвимостей на бесплатной основе, находящиеся в свободном доступе;

нарушителя, обладающим усиленным базовым (средним) потенциалом - возможности уровня группы лиц/организации, подразумевается, что имеют возможность проводить анализ кода прикладного программного обеспечения, самостоятельно находить в нем уязвимости и использовать их, а также могут разрабатывать и использовать специальные средства эксплуатации уязвимостей;

нарушителя, обладающим высоким потенциалом - возможности уровня предприятия/группы предприятий/государства, предполагается, что имеют возможность разрабатывать и использовать специальные средства эксплуатации уязвимостей, а также могут вносить закладки в программно-техническое обеспечение системы, проводить специальные исследования и применять специализированные средства проникновения и добывания информации.

Возможные потенциалы нарушителей и соответствующие им возможности приведены в приложении № 1.

Характер и объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации следующих нарушителей к реализации угроз различного типа (например, утечки информации по техническим каналам утечки информации):

1) внешний нарушитель с высоким потенциалом - специальные службы иностранных государств (нарушитель 1);

2) внешний нарушитель со средним потенциалом - преступные (хакерские) группы (нарушитель 2);

3) внутренний нарушитель с высоким потенциалом. Нарушители данной категории не рассматриваются в настоящей Модели угроз, так как предполагается, что данная категория внутренних нарушителей имеет возможности уровня предприятия/группы предприятий/государства, которые обладают большим финансированием, высоким потенциалом, знаниями и навыками для реализации угроз безопасности (например, проводить специальные исследования и применять специализированные средства проникновения и добывания информации).

Исходя из приложения № 1, настоящей Модели угроз, актуальными нарушителями являются:

1) внешний нарушитель с усиленным базовым (средним) потенциалом:

разработчики ИСПДн и программного обеспечения - нарушитель 4.

2) внешний нарушитель с базовым (низким) потенциалом:

физическое лицо, не являющееся служащим министерства – нарушитель 3;

бывшие работники (пользователи) - нарушитель 8.

3) внутренний нарушитель с усиленным базовым (средним) потенциалом:

администратор ИСПДн - нарушитель 6;

администратор безопасности - нарушитель 7.

4) внутренний нарушитель с базовым (низким) потенциалом:

лица, имеющие санкционированный доступ к рабочим местам пользователей (обслуживающий персонал) - нарушитель 5;

7. Анализ угроз безопасности информации, обрабатываемой в ИСПДн

В ИСПДн требуется обеспечить доступность и целостность защищаемой информации.

В соответствии с нормативными документами ФСТЭК России возможно возникновение или умышленная реализация несанкционированного доступа к информации.

При обработке информации в ИСПДн за счет реализации ТКУИ возникновение угроз безопасности информации невозможно.

Угрозы несанкционированного доступа к информации.

Угрозы непосредственного доступа к информации. Возможные угрозы непосредственного доступа:

угрозы, направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, перемещение, форматирование носителей информации и т.п.) прикладной программы, с применением специальных программ для осуществления НСД;

угрозы внедрения вредоносных программ.

Угрозы удаленного доступа. Возможные угрозы удаленного доступа:

реализация отказа в обслуживании;

угрозы внедрения вредоносных программ.

Анализ возможных угроз.

В качестве исходного перечня возможных уязвимостей и угроз безопасности информации используется банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

Угрозы утечки информации по техническим каналам характеризуются высокой стоимостью оборудования, необходимого для их реализации, и высокой квалификацией нарушителя. Цели и задачи ИСПДн, характер и объем защищаемой информации, хранимой и обрабатываемой в ИСПДн, являются недостаточными для мотивации нарушителя к реализации угроз, связанных с техническими каналами утечки информации. Исходя из этого, угрозы связанные с утечкой информации по техническим каналам являются неактуальными.

Технологии, не применимые в ИСПДн:

виртуализация;

беспроводной доступ;

мобильные технические средства;

грид-система;

суперкомпьютер;

гипервизор;

хранилища больших данных;

облачные технологии;

промышленные роботы;

WSDL-интерфейс;

утечка информации с неподключенных к сети Интернет компьютеров;

одноразовые пароли;

АСУ ТП;

станки ЧПУ.

Перечень возможных угроз безопасности информации и определение их актуальности в ИСПДн представлен в приложении № 3.

По каждому виду угрозы, экспертным путем (опрос специалистов) определена опасность (ущерб) в соответствии с правилами в таблице 4.

Таблица 4

Правила определения опасности (ущерба) угрозы безопасности информации

Опасность угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

вероятность реализации угрозы (в виде вербальной градации показателя о частоте (вероятности) реализации угрозы безопасности информации и соответствующего числового коэффициента Y2) в соответствии с правилами в таблице 5.

Таблица 5

Правила определения частоты (вероятности) реализации угрозы безопасности информации

Вероятность (Y2)	
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

1.4.1. Результаты изучения вероятности реализации угроз и опасности угроз приведены в приложении № 3.

1.4.2. С учетом полученных числовых коэффициентов Y1 и Y2 по каждому виду угрозы безопасности информации рассчитан числовой коэффициент реализуемости угрозы Y по формуле (1) и определена вербальная интерпретация реализуемости конкретной угрозы безопасности информации в соответствии с формулами в таблице 6.

$$Y = (Y1+Y2)/20$$

Таблица 6

Вербальная интерпретация определения реализуемости угрозы безопасности информации

Значение числового коэффициента реализуемости угрозы Y	Возможность реализации угрозы
0 ≤ Y ≤ 0,3	Низкая
0,3 <Y ≤ 0,6	Средняя
0,6 <Y ≤ 0,8	Высокая
Y> 0,8	Очень высокая

1.4.3. При определении степени опасности угроз утечки информации по техническим каналам связи учитывались границы контролируемой зоны (КЗ) и размещение технических средств.

1.4.4. Определена актуальность угроз безопасности информации на основании коэффициента реализуемости угрозы (Y) и показателя опасности угрозы по каждому ее виду, сделан вывод об актуальности угроз в соответствии с правилами в таблице 7.

Таблица 7

Правила определения актуальности угрозы безопасности информации

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

8. Актуальные угрозы

В результате проведенных мероприятий по анализу и выявлению актуальных угроз безопасности информации, сведений, содержащихся в ИСПДн, и структурно-функциональных особенностей ИСПДн, было установлено экспертным путем, что угрозы 1-го типа и 2-го типа не являются актуальными. Так как, реализация угроз в данной ИСПДн, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении считается маловероятной, ввиду обработки в ИСПДн информации, имеющей меньшую ценность (или стоимость), чем затраты на ее получение, а также использования в ИСПДн лицензионного системного программного обеспечения, сертифицированного программного обеспечения, сертифицированного средства антивирусной защиты.

Выявленные актуальные угрозы безопасности информации в ИСПДн относятся к угрозам 3-го типа: угрозы, не связанные с

наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Таким образом, согласно приложению № 3, приведенной в настоящей Модели угроз было выявлено 120 актуальных угроз безопасности. Актуальные угрозы безопасности информации в ИСПДн приведены в таблице 8.

Таблица 8

Актуальные угрозы безопасности информации в ИСПДн

№ п/п	Угроза	Тип угроз
1.	Угроза воздействия на программы с высокими привилегиями	Угрозы 3-го типа
2.	Угроза восстановления аутентификационной информации	Угрозы 3-го типа
3.	Угроза восстановления предыдущей уязвимой версии BIOS	Угрозы 3-го типа
4.	Угроза деструктивного изменения конфигурации/ среды окружения программ	Угрозы 3-го типа
5.	Угроза деструктивного использования декларированного функционала BIOS	Угрозы 3-го типа
6.	Угроза длительного удержания вычислительных ресурсов пользователями	Угрозы 3-го типа
7.	Угроза доступа к локальным файлам сервера при помощи URL	Угрозы 3-го типа
8.	Угроза доступа/перехвата/изменения HTTP cookies	Угрозы 3-го типа
9.	Угроза загрузки нештатной операционной системы	Угрозы 3-го типа
10.	Угроза заражения DNS-кеша	Угрозы 3-го типа
11.	Угроза избыточного выделения оперативной памяти	Угрозы 3-го типа
12.	Угроза изменения компонентов системы	Угрозы 3-го типа
13.	Угроза искажения XML-схемы	Угрозы 3-го типа
14.	Угроза искажения вводимой и выводимой на периферийные устройства информации	Угрозы 3-го типа
15.	Угроза использования альтернативных путей доступа к ресурсам	Угрозы 3-го типа
16.	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Угрозы 3-го типа

17.	Угроза использования механизмов авторизации для повышения привилегий	Угрозы 3-го типа
18.	Угроза использования поддельных цифровых подписей BIOS	Угрозы 3-го типа
19.	Угроза использования слабостей протоколов сетевого/локального обмена данными	Угрозы 3-го типа
20.	Угроза исследования механизмов работы программы	Угрозы 3-го типа
21.	Угроза исследования приложения через отчёты об ошибках	Угрозы 3-го типа
22.	Угроза межсайтового скриптинга	Угрозы 3-го типа
23.	Угроза межсайтовой подделки запроса	Угрозы 3-го типа
24.	Угроза нарушения изоляции среды исполнения BIOS	Угрозы 3-го типа
25.	Угроза нарушения целостности данных кэша	Угрозы 3-го типа
26.	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Угрозы 3-го типа
27.	Угроза невозможности управления правами пользователей BIOS	Угрозы 3-го типа
28.	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Угрозы 3-го типа
29.	Угроза некорректного задания структуры данных транзакции	Угрозы 3-го типа
30.	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угрозы 3-го типа
31.	Угроза некорректного использования функционала программного и аппаратного обеспечения	Угрозы 3-го типа
32.	Угроза неправомерного ознакомления с защищаемой информацией	Угрозы 3-го типа
33.	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Угрозы 3-го типа
34.	Угроза неправомерных действий в каналах связи	Угрозы 3-го типа
35.	Угроза несанкционированного восстановления удалённой защищаемой информации	Угрозы 3-го типа
36.	Угроза несанкционированного выключения или обхода	Угрозы 3-го типа

	механизма защиты от записи в BIOS	
37.	Угроза несанкционированного доступа к аутентификационной информации	Угрозы 3-го типа
38.	Угроза несанкционированного изменения аутентификационной информации	Угрозы 3-го типа
39.	Угроза несанкционированного использования привилегированных функций BIOS	Угрозы 3-го типа
40.	Угроза несанкционированного копирования защищаемой информации	Угрозы 3-го типа
41.	Угроза несанкционированного редактирования реестра	Угрозы 3-го типа
42.	Угроза несанкционированного создания учётной записи пользователя	Угрозы 3-го типа
43.	Угроза несанкционированного удаления защищаемой информации	Угрозы 3-го типа
44.	Угроза несанкционированного управления буфером	Угрозы 3-го типа
45.	Угроза несанкционированного управления указателями	Угрозы 3-го типа
46.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угрозы 3-го типа
47.	Угроза обнаружения хостов	Угрозы 3-го типа
48.	Угроза обхода некорректно настроенных механизмов аутентификации	Угрозы 3-го типа
49.	Угроза опосредованного управления группой программ через совместно используемые данные	Угрозы 3-го типа
50.	Угроза определения типов объектов защиты	Угрозы 3-го типа
51.	Угроза определения топологии вычислительной сети	Угрозы 3-го типа
52.	Угроза отключения контрольных датчиков	Угрозы 3-го типа
53.	Угроза перебора всех настроек и параметров приложения	Угрозы 3-го типа
54.	Угроза передачи данных по скрытым каналам	Угрозы 3-го типа
55.	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Угрозы 3-го типа
56.	Угроза переполнения целочисленных переменных	Угрозы 3-го типа

57.	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угрозы 3-го типа
58.	Угроза перехвата данных, передаваемых по вычислительной сети	Угрозы 3-го типа
59.	Угроза перехвата привилегированного потока	Угрозы 3-го типа
60.	Угроза перехвата привилегированного процесса	Угрозы 3-го типа
61.	Угроза повреждения системного реестра	Угрозы 3-го типа
62.	Угроза повышения привилегий	Угрозы 3-го типа
63.	Угроза подбора пароля BIOS	Угрозы 3-го типа
64.	Угроза подделки записей журнала регистрации событий	Угрозы 3-го типа
65.	Угроза подмены резервной копии программного обеспечения BIOS	Угрозы 3-го типа
66.	Угроза подмены содержимого сетевых ресурсов	Угрозы 3-го типа
67.	Угроза подмены субъекта сетевого доступа	Угрозы 3-го типа
68.	Угроза получения предварительной информации об объекте защиты	Угрозы 3-го типа
69.	Угроза преодоления физической защиты	Угрозы 3-го типа
70.	Угроза приведения системы в состояние «отказ в обслуживании»	Угрозы 3-го типа
71.	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
72.	Угроза программного сброса пароля BIOS	Угрозы 3-го типа
73.	Угроза пропуска проверки целостности программного обеспечения	Угрозы 3-го типа
74.	Угроза сбоя обработки специальным образом изменённых файлов	Угрозы 3-го типа
75.	Угроза сбоя процесса обновления BIOS	Угрозы 3-го типа
76.	Угроза удаления аутентификационной информации	Угрозы 3-го типа
77.	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угрозы 3-го типа

78.	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угрозы 3-го типа
79.	Угроза утраты вычислительных ресурсов	Угрозы 3-го типа
80.	Угроза утраты носителей информации	Угрозы 3-го типа
81.	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
82.	Угроза форматирования носителей информации	Угрозы 3-го типа
83.	Угроза «форсированного веб-браузинга»	Угрозы 3-го типа
84.	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
85.	Угроза эксплуатации цифровой подписи программного кода	Угрозы 3-го типа
86.	Угроза перехвата исключения/сигнала из привилегированного блока функций	Угрозы 3-го типа
87.	Угроза «кражи» учётной записи доступа к сетевым сервисам	Угрозы 3-го типа
88.	Угроза наличия механизмов разработчика	Угрозы 3-го типа
89.	Угроза неправомерного шифрования информации	Угрозы 3-го типа
90.	Угроза скрытного включения вычислительного устройства в состав бот-сети	Угрозы 3-го типа
91.	Угроза распространения «почтовых червей»	Угрозы 3-го типа
92.	Угроза «спама» веб-сервера	Угрозы 3-го типа
93.	Угроза «фарминга»	Угрозы 3-го типа
94.	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Угрозы 3-го типа
95.	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Угрозы 3-го типа
96.	Угроза несанкционированного использования системных и сетевых утилит	Угрозы 3-го типа
97.	Угроза несанкционированной модификации защищаемой информации	Угрозы 3-го типа

98.	Угроза отказа подсистемы обеспечения температурного режима	Угрозы 3-го типа
99.	Угроза физического устаревания аппаратных компонентов	Угрозы 3-го типа
100.	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угрозы 3-го типа
101.	Угроза несанкционированного воздействия на средство защиты информации	Угрозы 3-го типа
102.	Угроза подмены программного обеспечения	Угрозы 3-го типа
103.	Угроза маскирования действий вредоносного кода	Угрозы 3-го типа
104.	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Угрозы 3-го типа
105.	Угроза хищения аутентификационной информации из временных файлов cookie	Угрозы 3-го типа
106.	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Угрозы 3-го типа
107.	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Угрозы 3-го типа
108.	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угрозы 3-го типа
109.	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Угрозы 3-го типа
110.	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Угрозы 3-го типа
111.	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Угрозы 3-го типа
112.	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Угрозы 3-го типа
113.	Угроза перехвата управления информационной системой	Угрозы 3-го типа
114.	Угрозы выявления или подбора паролей	Угрозы 3-го типа

115.	Угроза сбоя системы электроснабже-ния	Угрозы 3-го типа
116.	Угроза использования не учтенных отчуждаемых носителей информации	Угрозы 3-го типа
117.	Угроза вывода из строя автоматизированные рабочие места, сервера или каналы связи	Угрозы 3-го типа
118.	Угроза несанкционированного отключения средств антивирусной защиты информации	Угрозы 3-го типа
119.	Угроза утраты, кражи носителей информации содержащих ключи электронной подписи	Угрозы 3-го типа
120.	Угроза неантропогенно-го (стихийного) характера, например удары молнии, пожары, наводнения и т.п.	Угрозы 3-го типа

Приложение № 1
к модели угроз безопасности информации при ее обработке в ИСПДн
ГАПОУ«Педколледж» г.Орска

Возможные потенциалы нарушителей и соответствующие им возможности

Субъект	**нарушителя**	**Потенциал нарушителей**	**Предположения об имеющихся возможностях по реализации угроз безопасности информации**	**Пр**
циальные службы иностранных государств	Внешний	Высокий	Обладают всеми возможностями нарушителей с базовым и средним потенциалами. Могут осуществить несанкционированный доступ к информационной системе из сети **связи общего пользования и (или) сетям международного информационного обмена** (незащищенных организационными мерами). Имеют возможность получить доступ к системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам ИСПДн для преднамеренного внесения в нее закладок и уязвимостей. Могут получить информацию об уязвимостях информационной системы путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) с использованием специально разработанных технических и программных средств. Могут самостоятельно создавать и применять специальные технические средства для добывания информации из ИСПДн (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.	Ха **Высо подгото возмож**

Преступные (хакерские) группы	Внешний	Средний	Обладают всеми возможностями нарушителей с базовым потенциалом. Могут осуществить несанкционированный доступ к информационной системе из сети **связи общего пользования и (или) сетям международного информационного обмена.** Могут получить **информацию** об уязвимостях информационной системы с использованием специальных технических и программных средств. Имеют возможность создания методов и средств реализации угроз безопасности информации и реализации угроз с применением специально разработанных технических и программных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Могут быть осведомлены о мерах защиты информации, применяемых в ИСПДн. Могут получить информацию об уязвимостях информационной системы или её отдельных компонентов (программное обеспечение) путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонент общесистемного ПО.	Ха **Высо подгото возмож Осущ учет дей**
зическое лицо, не являющийся служащим министерства	Внешний	Низкий	Могут получить информацию об уязвимостях отдельных компонентов (программном обеспечении) информационной системы, опубликованных в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках. Не исключено, что может самостоятельно создавать методы и средства реализации угроз на основе полученной из общедоступных источников информации. **Может приобрести доступное в свободной продаже ПО, необходимое для реализации атаки.**	Неса (или) в прикла управле браузер прикла специал

				Возде администр администр системы персонал
работчики ИСПДн (обеспечивающие техническую поддержку)	Внешний	Средний	Обладают всеми возможностями нарушителей с базовым потенциалом. Могут быть осведомлены о мерах защиты информации, применяемых в ИСПДн. Могут получить информацию об уязвимостях информационной системы или её отдельных компонентов (программное обеспечение) путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонент общесистемного ПО. Осведомлены о структурно-функциональных характеристиках и особенностях функционирования информационной системы.	Неса (или) в приклад управле браузер приклад специал Возде безопасн информа Возде систему програм непредн действи закладок
Лица, имеющие санкционированный доступ к рабочим местам пользователей и серверам на которых размещена ИСПДн, но не имеющие доступа к информации (обслуживающий персонал (охрана,	нутренний	Низкий	Могут получить информацию об уязвимостях отдельных компонентов (программном обеспечении) информационной системы, опубликованных в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках. Могут самостоятельно создавать методы и средства реализации угроз на основе полученной из общедоступных источников	

работники административно-хозяйственных служб))			информации.	
инистратор ИСПДн	нутренний	Средний	Обладают всеми возможностями нарушителей с базовым потенциалом. Могут быть осведомлены о мерах защиты информации, применяемых в ИСПДн. Могут получить информацию об уязвимостях информационной системы или её отдельных компонентов (программное обеспечение) путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонент общесистемного ПО. Осведомлены о структурно-функциональных характеристиках и особенностях функционирования информационной системы.	Неса (или) в приклад управле браузер приклад специал Возде систему програм непредн действи вредоно уязвимо Возде админис админис системы Неса (или) в общесис системы операци системы
Администратор безопасности	нутренний	Средний	Обладают всеми возможностями нарушителей с базовым потенциалом. Могут быть осведомлены о мерах защиты информации, применяемых в ИСПДн. Могут получить информацию об уязвимостях информационной системы или её отдельных компонентов (программное обеспечение) путем проведения, с использованием имеющихся в свободном	Неса (или) в приклад управле браузер приклад специал

			доступе программных средств, анализа кода прикладного ПО и отдельных програмных компонент общесистемного ПО. Осведомлены о структурно-функциональных характеристиках и особенностях функционирования информационной системы.	Неса (или) в общесис системы операци системы Возде админис системы Возде систему програм непредн действи вредоно уязвимо
вшие работники (пользователи)	Внешний	Низкий	Могут получить информацию об уязвимостях отдельных компонентов (программном обеспечении) информационной системы, опубликованных в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках. Могут самостоятельно создавать методы и средства реализации угроз на основе полученной из общедоступных источников информации.	Возде админис системы персона

Приложение № 2

к модели угроз безопасности информации при ее обработке в ИСПДн
ГАПОУ «Педколледжа» г. Орска

Анализ уточненных возможностей нарушителей и направления атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обосн
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	Объективные предпосылки для р – обслуживающий персонал функционирование ИСПДн; – воздействие на пользователей И – базы вирусных сигнатур регуля но приняты меры по обеспечени – в помещениях, в которых информации, невозможно нахожден – ответственный за обеспеч администраторы ИС назначаются из – работа пользователей ИС регла – используются сертифицирован – проводится обучение пользов безопасности информации и преду несоблюдение.
1.2	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Неактуально	Отсутствуют объективные предп – работа пользователей ИС регла – проводится обучение пользов безопасности информации и преду несоблюдение; – сведения о физических мер размещена ИС, доступны ограничен
1.3	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	Объективные предпосылки для р ремонт, обслуживание и сопров программно-технических средств выполняться не доверенными лицам но приняты меры по обеспечени ответственный за обеспече администраторы ИС назначаются из работа пользователей ИС регламе проводится обучение пользова

			безопасности информации и преду несоблюдение; программные, технические, про числе и СЗИ, ИС настроены в со безопасности информации; используются сертифицированны пользователи ИС не имеют во установки, изменения настроек име без контроля со стороны ответств информации
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Неактуально	Не осуществляется обработка сведе тайну, а также иных сведений, кото реализации возможности. Высокая стоимость и сложность под
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Неактуально	Не осуществляется обработка сведе тайну, а также иных сведений, кото реализации возможности
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	Неактуально	Не осуществляется обработка сведе тайну, а также иных сведений, кото реализации возможности

Приложение № 3
к модели угроз безопасности информации при ее обработке в ИСПДн
ГАПОУ «Педколледж» г.Орска

Перечень возможных угроз безопасности информации и определение их актуальности в ИСПДн

Идентификатор угрозы	Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Уровень исходной защищенности - Y1 (табл. 3)	Возможность реализации угрозы Y2 (табл. 10)	Коэффициент реализуемости угрозы Y(табл. 11)	Во... ре... уг... (т...
Угрозы из bdu.fstec.ru								
УБИ.1	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы	10	0	0.5	ср...
УБИ.2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: - сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; - привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы.	Внешний нарушитель со средним потенциалом	Сетевой трафик	10	0	0.5	ср...

УБИ.3	Угроза анализа криптографичес-ких алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	10	0	0.5	ср
УБИ.4	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	0	0.5	ср
УБИ.5	Угроза внедрения вредоносного кода в BIOS	Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	0	0. 5	ср

УБИ.6	Угроза внедрения кода или данных	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. Данная угроза обусловлена: – наличием уязвимостей программного обеспечения; – слабостями мер антивирусной защиты и разграничения доступа; – наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств). Реализация данной угрозы возможна: – в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; – при наличии у него привилегий установки программного обеспечения; – в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)	Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	ср
УБИ.7	Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: – обладания дискредитируемой программой повышенными привилегиями в системе; – осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; – нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик	10	2	0.6	ср

УБИ.8	Угроза восстановления аутентификационной информации	Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: – время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; – восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную».	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	10	2	0.6	ср
УБИ.9	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности осуществления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): – на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; – в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; – публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; – происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); – пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию.	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	2	0.6	ср

УБИ.10	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины	10	0	0.5	ср
УБИ.11	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети. Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных – сведения о MAC-адресах беспроводных клиентов доступны всем участникам сетевого взаимодействия. Реализация данной угрозы возможна при условии подключения нарушителем к беспроводной сети устройства, MAC-адрес которого будет полностью совпадать с MAC-адресом дискредитируемого санкционированного клиента	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел	10	0	0.5	ср
УБИ.12	Угроза деструктивного изменения конфигурации/ среды окружения программ	Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	10	2	0.6	ср

УБИ.13	Угроза деструктивного использования декларированного функционала BIOS	Угроза заключается в возможности неправомерного использования декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения BIOS/UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки целостности памяти, программного обеспечения управления RAID-контроллером и т.п.). Реализации данной угрозы может способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.14	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	5	0.75	Вы
УБИ.15	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: – наличие у нарушителя прав доступа к некоторым объектам файловой системы; – отсутствие проверки вводимых пользователем данных; – наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы	10	0	0.5	ср

УБИ.16	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе.	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	10	2	0.6	ср
УБИ.17	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов: отсутствием проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	10	5	0.75	Вы
УБИ.18	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	2	0.6	ср

УБИ.19	Угроза заражения DNS-кеша	Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	2	0.6	ср
УБИ.20	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	Внутренний нарушитель с низким потенциалом	Облачная система, виртуальная машина	10	0	0.5	ср

УБИ.21	Угроза злоупотребления доверием потребителей облачных услуг	Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки)	Внешний нарушитель с низким потенциалом	Облачная система	10	0	0. 5	ср
УБИ.22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.23	Угроза изменения компонентов системы	Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе.	Внутренний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	10	0	0.5	ср

УБИ.24	Угроза изменения режимов работы аппаратных элементов компьютера	Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: – за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; – за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; – за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки BIOS/UEFI.	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	0	0. 5	ср
УБИ.25	Угроза изменения системных и глобальных переменных	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0. 5	ср

УБИ.26	Угроза искажения XML-схемы	Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями механизма сетевого взаимодействия открытых систем. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к сетевому трафику, передаваемому между клиентом и сервером и отсутствии проверки целостности XML-схемы со стороны дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	2	0.6	ср
УБИ.27	Угроза искажения вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	10	5	0.75	вы

УБИ.28	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: – возможности ввода произвольных данных в адресную строку; – сведений о пути к защищаемому ресурсу; – возможности изменения интерфейса ввода входных данных	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	10	2	0.6	Ср
УБИ.29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Угроза заключается в возможности существенного снижения производительности вычислительного поля суперкомпьютера и эффективности выполнения на нём текущих параллельных вычислений из-за потребления вычислительных ресурсов суперкомпьютера «паразитными» процессами («процессами-потомками» предыдущих заданий или процессами, запущенными вредоносным программным обеспечением). Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением. Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера	10	0	0.5	ср

УБИ.30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: – наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; – успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	10	2	0.6	Ср
УБИ.31	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср

УБИ.32	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	Внешний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.33	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: – дискредитируемая система принимает входные данные от нарушителя; – нарушитель обладает возможностью управления одним или несколькими параметрами входных данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	10	0	0.5	ср
УБИ.34	Угроза использования слабостей протоколов сетевого/локального обмена данными	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср

УБИ.35	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы	Внешний нарушитель с высоким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	0	0.5	ср
УБИ.36	Угроза исследования механизмов работы программы	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: – наличия у нарушителя доступа к исходным файлам программы; – наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	10	2	0.6	ср
УБИ.37	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	10	2	0.6	ср

УБИ.38	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Угроза заключается в возможности временного возникновения состояния типа «отказ в обслуживании» у хранилища больших данных. Данная угроза обусловлена постоянным трудно контролируемым заполнением занятого дискового пространства за счёт данных, непрерывно поступающих из различных информационных источников, и слабостями технологий доступа и хранения информации в хранилищах больших данных. Реализация данной угрозы возможна при условии мгновенного (текущего) превышения скорости передачи данных над скоростью их сохранения (в силу недостаточности пропускной способности канала связи или скорости выделения свободного пространства и сохранения на него поступающих данных) или при условии временного отсутствия свободного места в хранилище (в силу некорректного управления хранилищем или в результате осуществления нарушителем деструктивного программного воздействия на механизм контроля за заполнением хранилища путём изменения параметров или логики его работы)	Внутренний нарушитель с низким потенциалом	Информационная система	10	0	0. 5	ср
УБИ.39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей	Внешний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	0	0. 5	ср

УБИ.40	Угроза конфликта юрисдикций различных стран	Угроза заключается в возможности отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства стран, резиденты которых участвуют в оказании облачных услуг. Данная угроза обусловлена тем, что в зависимости от особенностей законодательства различных стран, резиденты которых участвуют в оказании облачных услуг, при обеспечении информационной безопасности могут использоваться правовые меры различных юрисдикций. Реализация данной угрозы возможна при условии того, что на обеспечение информационной безопасности в ходе оказания облачных услуг накладываются правовые меры различных юрисдикций, противоречащих друг другу в ряде вопросов	Внешний нарушитель с низким потенциалом	Облачная система	10	0	0. 5	ср
УБИ.41	Угроза межсайтового скриптинга	Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.42	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	10	2	0.6	Ср

УБИ.43	Угроза нарушения доступности облачного сервера	Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, облачный сервер	10	0	0. 5	ср
УБИ.44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальная машина, гипервизор	10	0	0. 5	Ср

УБИ.45	Угроза нарушения изоляции среды исполнения BIOS	Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: – со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; – со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	0	0.5	ср
УБИ.46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя	10	0	0. 5	ср

УБИ.47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). Данная угроза обусловлена слабостью технологий грид-вычислений – производительность грид-системы имеет сильную зависимость от загруженности каналов связи, что является следствием максимальной территориальной распределённости вычислительного модуля грид-системы среди всех типов информационных систем. Реализация данной угрозы возможна при условии недостаточного контроля за состоянием отдельных узлов грид-системы со стороны диспетчера задач грид-системы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Грид-система, сетевой трафик	10	0	0. 5	ср
УБИ.48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: – к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; – к нарушению целостности программ, установленных на виртуальных машинах; – к нарушению доступности ресурсов виртуальных машин; – к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы).	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина	10	0	0.5	ср

УБИ.49	Угроза нарушения целостности данных кеша	Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными. Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	2	0.6	ср
УБИ.50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультиформатной информации в хранилищах больших данных. Реализация данной угрозы возможна при условии, что дополнительная служебная информация о данных по какой-либо причине не соответствует их фактическому содержимому, или в хранилище больших данных не реализованы методы обработки данных получаемого формата	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные	10	0	0.5	ср
УБИ.51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания («ждущего режима работы», «гибернации» и др.)	Внутренний нарушитель с низким потенциалом	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр	10	0	0.5	ср

УБИ.52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг	Внешний нарушитель с низким потенциалом	Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение	10	0	0.5	ср
УБИ.53	Угроза невозможности управления правами пользователей BIOS	Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами. Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	0	0.5	ср

УБИ.54	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы	10	0	0.5	ср
УБИ.55	Угроза незащищённого администрирования облачных услуг	Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, функционирующие в облачной среде, путём перехвата управления над облачной инфраструктурой через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями облачных услуг данных (в том числе аутентификационных данных), а также уязвимостями небезопасных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, рабочая станция, сетевое программное обеспечение	10	0	0.5	ср

УБИ.56	Угроза некачественного переноса инфраструктуры в облако	Угроза заключается в возможности снижения реального уровня защищённости иммигрирующей в облако информационной системы из-за ошибок, допущенных при миграции в ходе преобразования её реальной инфраструктуры в облачную. Данная угроза обусловлена тем, что преобразование даже части инфраструктуры информационной системы в облачную зачастую требует проведения серьёзных изменений в такой инфраструктуре (например, в политиках безопасности и организации сетевого обмена данными). Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако.	Внешний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, облачная система	10	0	0.5	ср
УБИ.57	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. Данная угроза обусловлена осуществлением дублирования (дву- или многократного) данных на различных вычислительных узлах, входящих в состав хранилища больших данных, с целью повышения скорости доступа к этим данным при большом количестве запросов чтения/записи. При этом данная операция является внутренней функцией и «непрозрачна» для конечных пользователей и администраторов хранилища больших данных. Реализация данной угрозы возможна при условии недостаточности мер по контролю за автоматически создаваемыми копиями информации, применяемых в хранилище больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные	10	0	0.5	ср

УБИ.58	Угроза неконтролируемого роста числа виртуальных машин	Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура	10	0	0.5	ср
УБИ.59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сервер	10	2	0.6	Ср
УБИ.60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Угроза заключается в возможности удаления из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора. Данная угроза обусловлена слабостями механизма автоматического удаления данных, не отвечающих определённым требованиям (предельный «срок жизни» в хранилище, конечная несогласованность с другими данными, создание копии в другом месте и т.п.). Реализация данной угрозы возможна при условии недостаточности реализованных в хранилище больших данных мер по контролю за автоматическим удалением данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные	10	0	0.5	ср

УБИ.61	Угроза некорректного задания структуры данных транзакции	Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом	Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое программное обеспечение	10	2	0.6	ср
УБИ.62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	2	0.6	ср
УБИ.63	Угроза некорректного использования функционала программного и аппаратного обеспечения	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	10	2	0.6	ср

УБИ.64	Угроза некорректной реализации политики лицензирования в облаке	Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	ср
УБИ.65	Угроза неопределённости в распределении ответственности между ролями в облаке	Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки облачной инфраструктуры и т. п. Возможность реализации данной угрозы повышается в случае использования облачных услуг, предоставляемых другими поставщиками (т.е. в случае использования схемы оказания облачных услуг с участием посредников)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	0	0.5	ср
УБИ.66	Угроза неопределённости ответственности за обеспечение безопасности облака	Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности	Внешний нарушитель с низким потенциалом	Облачная система	10	0	0.5	ср

УБИ.67	Угроза неправомерного ознакомления с защищаемой информацией	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, носители информации, объекты файловой системы	10	0	0.5	ср
УБИ.68	Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд API, используемого программным обеспечением. Реализация данной угрозы возможна в условиях наличия у нарушителя доступа к API и отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	10	2	0.6	ср
УБИ.69	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	Внешний нарушитель с низким потенциалом	Сетевой трафик	10	2	0.6	Ср

УБИ.70	Угроза непрерывной модернизации облачной инфраструктуры	Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться таковой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)	Внутренний нарушитель со средним потенциалом	Облачная инфраструктура	10	0	0. 5	ср
УБИ.71	Угроза несанкционированного восстановления удалённой защищаемой информации	Угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: – удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); – технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; – информация не хранилась в криптографически преобразованном виде	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Машинный носитель информации	10	0	0.5	ср

УБИ.72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Угроза заключается в возможности внедрения в BIOS/UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в BIOS/UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостями механизма обновления BIOS/UEFI, приводящими к переполнению буфера. Реализация данной угрозы возможна в одном из следующих условий: – выключенном механизме защиты BIOS/UEFI от записи; – успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства	10	0	0.5	ср
УБИ.74	Угроза несанкционированного доступа к аутентификационной информации	Угроза заключается в возможности извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	10	2	0.6	ср

УБИ.75	Угроза несанкционированного доступа к виртуальным каналам передачи	Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства	10	0	0.5	ср
УБИ.76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: – наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; – наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Гипервизор	10	0	0.5	ср

УБИ.77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные	10	0	0.5	ср
УБИ.78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина	10	0	0.5	ср

УБИ.79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина	10	0	0.5	ср
УБИ.80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальные устройства хранения, обработки и передачи данных	10	0	0.5	ср

УБИ.81	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Угроза заключается в возможности выполнения нарушителем сетевого входа на узел грид-системы с правами одной из учётных записей, соответствующей программным процессам системы управления заданиями, с последующим получением доступа к закрытой части криптографических сертификатов, используемых для установления связи в грид-системе. Данная угроза обусловлена наличием уязвимостей в клиенте грид-системы (клиентского программного обеспечения, устанавливаемого в узлах грид-системы), эксплуатация которых позволяет нарушителю осуществлять операции чтения и записи в объектах локальной файловой системы компьютера, отправку сигналов программным процессам (включая сигналы прекращения работы), операции чтения и записи в память программных процессов, соответствующих связующему программному обеспечению и грид-заданиям, открытия сетевых соединений в локальных и внешних узлах грид-системы. Реализация данной угрозы возможна при условии внедрения вредоносного программного кода в систему управления заданиями. Фактически наличие в узле грид-системы неизвестного его владельцу программного обеспечения (клиента грид-системы), проводящего неизвестные вычисления, является «черным ящиком», через который (путём эксплуатации уязвимостей или программных закладок) нарушитель может осуществить противоправные действия по отношению к хранящейся в узле грид-системы защищаемой информации (личной информации владельца узла)	Внешний нарушитель со средним потенциалом	Узлы грид-системы	10	0	0.5	ср
УБИ.82	Угроза несанкционированного доступа к сегментам вычислительного поля	Угроза заключается в возможности осуществления несанкционированного доступа нарушителя к исходным данным, промежуточным и окончательным результатам расчётов других пользователей суперкомпьютера, а также случайное или преднамеренное деструктивное воздействие процессов решения одних задач на процессы и результаты решения других вычислительных задач. Данная угроза обусловлена слабостями механизма разграничения доступа субъектов к сегментам вычислительных полей суперкомпьютера. Реализация данной угрозы возможна при выполнении задач различных пользователей суперкомпьютера на одном вычислительном поле суперкомпьютера	Внутренний нарушитель со средним потенциалом	Вычислительный узел суперкомпьютера	10	0	0.5	ср

УБИ.83	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2), используемых для авторизации пользователей при подключении к точке беспроводного доступа. Реализация данной угрозы возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации/ аутентификации беспроводных сетей, а также нахождения в точке приёма сигналов дискредитируемой беспроводной сети	Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	10	0	0.5	ср
УБИ.84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальные устройства хранения данных, виртуальные диски	10	0	0.5	ср

УБИ.85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, объекты файловой системы	10	0	0.5	ср
УБИ.86	Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	10	2	0.6	Ср
УБИ.87	Угроза несанкционированного использования привилегированных функций BIOS	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI	10	0	0.5	ср

УБИ.88	Угроза несанкционированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	10	0	0.5	ср
УБИ.89	Угроза несанкционированного редактирования реестра	Угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, использующее реестр, реестр	10	2	0.5	ср

УБИ.90	Угроза несанкционированного создания учётной записи пользователя	Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	2	0.6	ср
УБИ.91	Угроза несанкционированного удаления защищаемой информации	Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Метаданные, объекты файловой системы, реестр	10	0	0.5	Ср

УБИ.92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: – наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; – наличия подключения системы к сетям общего пользования (сети Интернет)	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	10	0	0.5	ср
УБИ.93	Угроза несанкционированного управления буфером	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср

УБИ.94	Угроза несанкционированного управления синхронизацией и состоянием	Угроза заключается в возможности изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния информационной системы (например, текущих значений глобальных переменных, наличия запущенных процессов и др.), или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.). Данная угроза основана на слабостях механизма управления синхронизацией и состоянием, позволяющих нарушителю вносить изменения в его работу в определённые промежутки времени, или отсутствии механизмов аутентификации и авторизации. Реализация данной угрозы возможна при условии наличия у нарушителя возможности: – контролировать состояние дискредитируемого приложения (этапы выполнения алгоритма) или промышленных роботов; – отслеживать моменты времени, когда дискредитируемое приложение временно прерывает свою работу с глобальными данными; – выполнить деструктивные действия в определённые моменты времени (например, внести изменения в файл с данными или изменить содержимое ячейки памяти)	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	10	0	0.5	ср
УБИ.95	Угроза несанкционированного управления указателями	Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср

УБИ.96	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённой облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, облачная система	10	0	0.5	ср
УБИ.97	Угроза несогласованности правил доступа к большим данным	Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Внутренний нарушитель с низким потенциалом	Хранилище больших данных	10	0	0.5	ср

УБИ.98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	5	0.75	вы
УБИ.99	Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср

УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). Данная угроза обусловлена в случае некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных. Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.101	Угроза общедоступности облачной инфраструктуры	Угроза заключается в возможности осуществления несанкционированного доступа к защищаемой информации одного потребителя облачных услуг со стороны другого. Данная угроза обусловлена тем, что из-за особенностей облачных технологий потребителям облачных услуг приходится совместно использовать одну и ту же облачную инфраструктуру. Реализация данной угрозы возможна в случае допущения ошибок при разделении элементов облачной инфраструктуры между потребителями облачных услуг, а также при изоляции их ресурсов и обособлении данных друг от друга	Внешний нарушитель со средним потенциалом	Объекты файловой системы, аппаратное обеспечение, облачный сервер	10	0	0.5	ср
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Угроза заключается в возможности опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные, файлы конфигурации и др.). Данная угроза обусловлена наличием слабостей в механизме контроля внесённых изменений в общие данные каждой из программ в группе. Реализация данной угрозы возможна в случае успешного перехвата нарушителем управления над одной из программ в группе программ, использующих общие данные	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	ср

УБИ.103	Угроза определения типов объектов защиты	Угроза заключается в возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (данный метод известен как «fingerprinting», с англ. «дактилоскопия»). Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз. Данная угроза обусловлена ошибками в параметрах конфигурации средств межсетевого экранирования, а также с отсутствием механизмов контроля входных и выходных данных. Реализация данной угрозы возможна в случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией дискредитируемой системы (документация на программные средства, стандарты передачи данных, спецификации и т.п.)	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср
УБИ.104	Угроза определения топологии вычислительной сети	Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика). Реализация данной угрозы возможна в случае наличия у нарушителя возможности подключения к исследуемой вычислительной сети и наличием специализированного программного обеспечения, реализующего функцию анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср

УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Угроза заключается в возможности отказа хранилищем больших данных в приёме входных данных неизвестного формата от легального пользователя. Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных. Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные	10	0	0.5	ср
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Угроза заключается в возможности значительного замедления работы терминальных сессий всех пользователей суперкомпьютера, вплоть до достижения всем суперкомпьютером состояния «отказ в обслуживании» при превышении максимально достижимой нагрузки на параллельную файловую систему суперкомпьютера. Данная угроза обусловлена значительным повышением числа и объёма сохраняемых на накопитель данных для некоторых вычислительных задач. Реализация данной угрозы возможна при условии интенсивного файлового ввода-вывода в кластерной файловой подсистеме суперкомпьютера, основанной на использовании параллельной файловой системы	Внутренний нарушитель с низким потенциалом	Система хранения данных суперкомпьютера	10	0	0.5	ср
УБИ.107	Угроза отключения контрольных датчиков	Угроза заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путём прерывания канала связи с контрольными датчиками, следящими за параметрами состояния системы, или нарушения работы самих датчиков. При этом система перестанет реагировать как на инциденты безопасности (если отключённые датчики являлись частью системы безопасности, например, датчики движения), так и на другие типы инцидентов (например, при отключении датчиков пожарной сигнализации, повышения давления в гидроагрегатах и др.). Данная угроза обусловлена слабостями мер защиты информации в автоматизированных системах управления технологическими процессами, а также наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна при условии получения доступа (физического или программного) к линиям связи системы безопасности с контрольными датчиками или к самим датчикам	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	0	0.5	ср

УБИ.108	Угроза ошибки обновления гипервизора	Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления. Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: – сбоев в процессе его обновления; – обновлений, в ходе которых внедряются новые ошибки в код гипервизора; – обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; – других инцидентов безопасности информации	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, гипервизор	10	0	0.5	ср
УБИ.109	Угроза перебора всех настроек и параметров приложения	Угроза заключается в возможности получения нарушителем доступа к дополнительному скрытому функционалу (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличии от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	10	2	0.6	Ср

УБИ.110	Угроза перегрузки грид-системы вычислительным и заданиями	Угроза заключается в возможности снижения пропускной способность ресурсных центров при отправке большого количества заданий одним пользователем (нарушителем) случайно или намеренно, что может сделать невозможной постановку заданий другими пользователями грид-системы в очередь на выполнение. Данная угроза обусловлена слабостями мер по контролю в грид-системе за количеством вычислительных заданий, запускаемых пользователями грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя прав на постановку заданий в очередь на выполнение грид-системой	Внутренний нарушитель с низким потенциалом	Ресурсные центры грид-системы	10	0	0.5	ср
УБИ.111	Угроза передачи данных по скрытым каналам	Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передаче управляющих команд путём её нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путём её маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография), использования скрытых пикселей («пикселей отслеживания») и т.п. Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при: – наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; – доступа к каналам передачи данных; – посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	10	0	0.5	Ср

УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Угроза заключается в возможности повреждения нарушителем исполнительных механизмов, заготовки и (или) обрабатывающего инструмента оборудования с числовым программным управлением путём передачи на него команд, приводящих к перемещению обрабатывающего инструмента за допустимые пределы (т.е. команд, запрещённых для оборудования с числовым программным управлением). Данная угроза обусловлена слабостями мер по защите оборудования с числовым программным управлением от выполнения запрещённых команд. Реализация данной угрозы возможна при наличии у нарушителя привилегий на передачу команд на оборудование с числовым программным управлением или возможности изменения команд, передаваемых легальным пользователем	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение	10	0	0.5	ср
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо) при выполнении следующих условий: – наличие в системе открытых сессий работы пользователей; – наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, аппаратное обеспечение	10	0	0.5	Ср

УБИ.114	Угроза переполнения целочисленных переменных	Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путём подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определённые типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; – возможности взаимодействия с входным интерфейсом дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств. Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	10	0	0.5	ср

УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: – наличие у нарушителя доступа к дискредитируемой вычислительную сети; – неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевой трафик	10	0	0.5	Ср
УБИ.117	Угроза перехвата привилегированного потока	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями (к привилегированному потоку данных), путём синхронного (вызов привилегированной функции, возвращающей неправильное значение) или асинхронного (создание обратных вызовов, манипулирование указателями и т.п.) деструктивного программного воздействия на него. Данная угроза обусловлена уязвимостями программного обеспечения, использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками (наличие ошибочных указателей, некорректное освобождение памяти и т.п.). Реализация данной угрозы возможна в следующих условиях: – в дискредитируемом приложении существуют участки кода, требующие исполнения с правами, превышающими права обычных пользователей; – нарушитель обладает привилегиями, позволяющими вносить изменения во входные данные дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	Ср

УБИ.118	Угроза перехвата привилегированного процесса	Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов. Реализация данной угрозы возможна при выполнении одного из условий: – успешного введения нарушителем некорректных данных, приводящих к переполнению буфера или к реализации некоторых типов программных инъекций; – наличия у нарушителя привилегий на запуск системных утилит, предназначенных для управления процессами	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	Ср
УБИ.119	Угроза перехвата управления гипервизором	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём эксплуатации уязвимостей консоли управления гипервизором. Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, гипервизор, консоль управления гипервизором	10	0	0.5	ср

УБИ.120	Угроза перехвата управления средой виртуализации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение	10	0	0.5	ср

УБИ.121	Угроза повреждения системного реестра	Угроза заключается в возможности нарушения доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр. Данная угроза обусловлена слабостями мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы. Реализация данной угрозы возможна при одном из условий: – возникновения ошибок в работе отдельных процессов или всей операционной системы; – наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, реестр	10	2	0.6	Ср
УБИ.122	Угроза повышения привилегий	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации). Реализация данной угрозы возможна при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение, информационная система	10	2	0.6	Ср

УБИ.123	Угроза подбора пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: – нарушитель может осуществить физический доступ к компьютеру и имеет возможность его перезагрузить; – нарушитель обладает специальным программным средством перебора паролей BIOS/UEFI и привилегиями в системе на установку и запуск таких средств	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.124	Угроза подделки записей журнала регистрации событий	Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: – технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; – технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	2	0.6	Ср

УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Угроза заключается в возможности осуществления нарушителем перехвата трафика беспроводной сети или других неправомерных действий путём легализации нарушителем собственного подключения к беспроводной сети в полуавтоматическом режиме (например, WPS) без ввода ключа шифрования. Данная угроза обусловлена слабостями процедуры аутентификации беспроводных устройств в ходе полуавтоматического подключения. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к беспроводной точке доступа, поддерживающей полуавтоматический режим подключения	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	0	0.5	ср
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Угроза заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического подключения точек беспроводного доступа или клиентского программного обеспечения к доверенным субъектам сетевого взаимодействия, подменённым нарушителем. Данная угроза обусловлена слабостями механизма аутентификации субъектов сетевого взаимодействия при беспроводном доступе. Реализация данной угрозы возможна в случае размещения нарушителем клиента или точки беспроводного доступа со специально сформированными параметрами работы (такими как MAC-адрес, название, используемый стандарт передачи данных и т.п.) в зоне доступности для дискредитируемых устройств беспроводного доступа	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка беспроводного доступа	10	0	0.5	ср
УБИ.127	Угроза подмены действия пользователя путём обмана	Угроза заключается в возможности нарушителя выполнения неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии (обмана пользователя, навязывание ложных убеждений) или технических методов (использование прозрачных кнопок, подмена надписей на элементах управления и др.) Данная угроза обусловлена слабостями интерфейса взаимодействия с пользователем или ошибками пользователя. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя прав на проведение нужных от него нарушителю операций	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	Ср

УБИ.128	Угроза подмены доверенного пользователя	Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и т.п.	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	0	0.5	Ср
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения BIOS/UEFI, предварительно подменённой нарушителем. Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в следующих условиях: – нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; – возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения. Реализация данной угрозы возможна при условии наличия у нарушителя прав на доступ к сетевым ресурсам и отсутствии у пользователя сети мер по обеспечению их целостности	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср

УБИ.131	Угроза подмены субъекта сетевого доступа	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср
УБИ.132	Угроза получения предварительной информации об объекте защиты	Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и др., путём проведения мероприятий по сбору и анализу доступной информации о системе. Данная угроза обусловлена наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы: – анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию (о трассировке стека, о конфигурации системы, о маршруте прохождения сетевых пакетов); – анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам). Данная угроза отличается от угрозы	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	10	2	0.6	Ср

		перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает						
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Угроза заключается в возможности раскрытия нарушителем сведений о географических перемещениях дискредитируемого пользователя в определённые промежутки времени, в том числе выявить место его работы, проживания и т.п. Получение таких сведений может использоваться нарушителем в дальнейшем для реализации угроз в информационных системах, доступ к которым имеет дискредитируемый пользователь. Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет. Реализация данной угрозы возможна при условии наличия у нарушителя доступа к идентификационными данным стационарных точек беспроводного доступа, с которыми в автоматическом режиме осуществляет взаимодействие беспроводное устройство дискредитируемого пользователя	Внешний нарушитель с низким потенциалом	Сетевой узел, метаданные	10	0	0.5	ср

УБИ.134	Угроза потери доверия к поставщику облачных услуг	Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невосполнимого оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику. Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок. Реализация данной угрозы возможна в случае обнародования единичных или множественных фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, повлёкших значительные убытки для его клиентов	Внутренний нарушитель со средним потенциалом	Объекты файловой системы, информационная система, иммигрированная в облако	10	0	0.5	ср
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе. Данная угроза обусловлена слабостями мер защиты информации, обрабатываемой в облачной системе. Реализация данной угрозы возможна в случае допущения поставщиком (некорректный выбор или настройка средств защиты) или потребителем (потеря пароля, электронного ключа, вход с небезопасной консоли) облачных услуг ошибок при обеспечении безопасности защищаемой информации	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, метаданные, объекты файловой системы	10	0	0.5	ср

УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Угроза заключается в возможности допуска ошибок при копировании защищаемой информации при распределённом хранении данных на различных узлах хранилища больших данных вследствие несогласованности их работы, влекущих за собой невозможность осуществления легальным пользователем доступа к блокам или ко всей защищаемой информации. Данная угроза обусловлена слабостями механизмов репликации данных, реализованных в узлах хранилища больших данных. Реализация данной угрозы возможна в условиях отключения или выведения из строя одного или нескольких узлов за счёт специальных программных воздействий на узлы хранилища больших данных, а также возникновения технических или программных сбоев в работе их компонентов	Внутренний нарушитель с низким потенциалом	Информационная система, узлы хранилища больших данных	10	0	0.5	ср
УБИ.137	Угроза потери управления облачными ресурсами	Угроза заключается в возможности нарушения договорных обязательств со стороны поставщика облачных услуг в отношении их потребителя из-за значительной сложности построения эффективной системы управления облачными ресурсами облачной системы, особенно использующей облачные ресурсы других поставщиков облачных услуг. Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг. Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется (или становится невозможным) из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика	Внешний нарушитель с высоким потенциалом	Сетевой трафик, объекты файловой системы	10	0	0.5	ср

УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Угроза заключается в возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако, со стороны поставщика облачных услуг из-за отсутствия у него сведений об особенностях управления конкретной системы, а также из-за отсутствия у потребителя облачных услуг, обладающего такими сведениями, возможности проводить весь комплекс работ по управлению инфраструктурой собственной системы в связи с её иммиграцией в облако. Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации. Реализация данной угрозы возможна в случаях передачи поставщику облачных услуг части функций управления системой потребителя облачных услуг (при миграции части или всей системы в облако)	Внутренний нарушитель со средним потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	0	0.5	ср
УБИ.139	Угроза преодоления физической защиты	Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)	Внешний нарушитель со средним потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	10	0	0.5	Ср

УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой. Данная угроза обусловлена тем, что для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	5	0.75	вы
УБИ.141	Угроза привязки к поставщику облачных услуг	Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)	Внутренний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	10	0	0.5	ср

УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Угроза заключается в возможности снижения качества облачных услуг (или даже отказа в их оказании конечным потребителям) из-за возникновения технических сбоев хотя бы у одного из поставщиков облачных услуг (входящих в цепь посредников при оказании облачных услуг их конечному потребителю), а также из-за возникновения существенных задержек или потерь в каналах передачи данных, арендуемых потребителем или поставщиками облачных услуг. Данная угроза обусловлена слабостями процедуры контроля за выполнением технического обслуживания и соблюдением режимов функционирования технических средств облачной информационной системы. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы		Системное программное обеспечение, аппаратное обеспечение, канал связи	10	0	0.5	ср
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	10	2	0.6	Ср

УБИ.144	Угроза программного сброса пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля. Данная угроза обусловлена слабостями мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI. Реализация данной угрозы возможна при условиях: – наличия в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля непосредственно из-под операционной системы; – наличия у нарушителя специальных программных средств, реализующих сброс пароля, а также прав в операционной системе для установки и запуска данных средств	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	10	2	0.6	ср
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения. Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов: – «ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); – «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	10	2	0.6	ср

УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Угроза заключается в возможности осуществления процессом нарушителя, функционирующем в вычислительном поле суперкомпьютера, считывания защищаемых данных из оперативной памяти, выделенной для параллельного (дискредитируемого) процесса, с использованием операций удалённого прямого доступа к памяти. Данная угроза обусловлена слабостями протокола прямого доступа к оперативной памяти, с помощью которого выполняется обращение к сегменту памяти, выделенному для удалённого параллельного процесса, функционирующего в вычислительном поле суперкомпьютера. Реализация данной угрозы возможна при условии успешного осуществления нарушителем доступа к входным/выходным данным параллельных процессов в вычислительном поле суперкомпьютера	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Вычислительные узлы суперкомпьютера, каналы передачи данных суперкомпьютера, системное программное обеспечение	10	0	0.5	ср
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Угроза заключается в возможности автоматического распространения на всю грид-систему несанкционированно полученных нарушителем на одном узле привилегий. Данная угроза обусловлена наличием уязвимостей в клиентском программном обеспечении грид-системы и слабостями в механизме назначения прав пользователям, реализованном в связующем программном обеспечении. Реализация данной угрозы возможна при условии успешного повышения нарушителем своих прав на одном узле грид-системы	Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы, узлы грид-системы, грид-система, сетевое программное обеспечение	10	0	0.5	ср
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Угроза заключается в возможности возникновения ситуаций, связанных с ошибками автоматического назначения пользователям прав доступа (наделение дополнительными полномочиями, ошибочное наследование, случайное восстановление «неактивных» учётных записей т.п.). Данная угроза обусловлена слабостями мер контроля за большим количеством (от тысячи, а в некоторых случаях и до нескольких миллионов) учётных записей пользователей со стороны администраторов безопасности. Реализация данной угрозы возможна при условии возникновения сбоев или ошибок в работе системы разграничения доступа хранилища больших данных		Информационная система, система разграничения доступа хранилища больших данных	10	0	0.5	ср

УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путём вызова сбоя в их работе за счёт внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных. Реализация данной угрозы возможна в условиях: – наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке; – успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное программное обеспечение	10	2	0.6	Ср
УБИ.150	Угроза сбоя процесса обновления BIOS	Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение BIOS/UEFI в результате нарушения процесса его обновления. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке повреждённой/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и совместимости)	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	10	2	0.5	ср
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Угроза заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера. Данная угроза обусловлена недостаточностью мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям. Реализация данной угрозы возможна при наличии у нарушителя сетевого доступа к исследуемому сетевому ресурсу и специальных программных средств сканирования сети	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой узел	10	0	0.5	ср

УБИ.152	Угроза удаления аутентификационной информации	Угроза заключается в возможности отказа легитимным пользователям в доступе к информационным ресурсам, а также в возможности получения нарушителем привилегий дискредитированного пользователя за счёт сброса (обнуления, удаления) его аутентификационной информации. Данная угроза обусловлена слабостями политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями пользователей. Реализация данной угрозы возможна при выполнении одного из следующих условий: – штатные средства работы с учётными записями пользователей обладают функционалом сброса аутентификационной информации, и нарушитель получил привилегии в дискредитируемой системе на использование данных средств; – нарушитель обладает специальным программным обеспечением, реализующим функцию сброса аутентификационной информации, и получил привилегии в дискредитируемой системе на использование данных средств	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	10	2	0.6	Ср
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объёмом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объём сетевых запросов, формируемых нарушителем. Данная угроза обусловлена слабостями мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов; – сведений о сетевом адресе дискредитируемой системы; – специального программного обеспечения, реализующего функции генерации сетевых пакетов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	10	0	0.5	Ср

УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI	10	2	0.6	ср
УБИ.155	Угроза утраты вычислительных ресурсов	Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за исчерпания нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов». Данная угроза обусловлена слабостями механизма контроля за распределением вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы; – привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе; – отсутствие у администраторов возможности: для техники «утечки ресурсов» – перезагрузки системы во время отправки нарушителем большого числа запросов на выделение ресурсов, а для техники «выделения ресурсов» – форсированного освобождения ресурсов, выделенных по запросам вредоносных процессов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	10	2	0.6	Ср

УБИ.156	Угроза утраты носителей информации	Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	Внутренний нарушитель с низким потенциалом	Носитель информации	10	2	0.5	Ср
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	10	2	0.6	Ср
УБИ.158	Угроза форматирования носителей информации	Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации. Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: – время, прошедшее после форматирования; – тип носителя информации; – тип файловой системы носителя; – интенсивность взаимодействия с носителем после форматирования и др.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Носитель информации	10	2	0.6	Ср

УБИ.159	Угроза «форсированного веб-браузинга»	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	10	2	0.6	ср
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля суперкомпьютера. Данная угроза обусловлена слабостями мер контроля за распределением вычислительных ресурсов суперкомпьютера при обработке задачи несколькими процессорами. Реализация данной угрозы возможна при условии выполнения суперкомпьютером специфичных вычислительных задач, в ходе которых генерируются межпроцессорные сообщения с большой интенсивностью	Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера	10	0	0.5	ср

УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: – дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; – дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); – нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение	10	2	0.6	Ср
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путём перехвата исключений/сигналов, сгенерированных участком программного кода, исполняемого с повышенными привилегиями (привилегированным блоком функций) и содержащего команды по управлению защищаемой информацией. Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа. Реализация данной угрозы возможна при следующих условиях: – дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java); – в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока); – нарушитель обладает правами, достаточными для перехвата программных исключений в системе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение	10	2	0.6	ср

УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Угроза заключается в возможности распространения негативных последствий от реализации угроз на физическом или виртуальном уровне облачной инфраструктуры на уровни управления и оркестровки, а также на все информационные системы, развёрнутые на базе дискредитированной облачной инфраструктуры. Данная угроза обусловлена невозможностью функционирования информационных систем в облаке при некорректной работе самой облачной инфраструктуры, а также зависимостью работоспособности верхних уровней облачной инфраструктуры от работоспособности нижних. Реализация данной угрозы возможна в случае приведения облачной инфраструктуры на физическом или виртуальном уровне облачной инфраструктуры в состояние «отказ в обслуживании»	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная инфраструктура, созданная с использованием технологий виртуализации	10	0	0.5	ср
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированности и др.	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	10	0	0.5	Ср
УБИ.166	Угроза внедрения системной избыточности	Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) из-за внедрения в него (в неё) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой)	Внутренний нарушитель со средним потенциалом	Программное обеспечение, информационная система, ключевая система информационной инфраструктуры	10	0	0.5	Ср

УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым	Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	0	0.5	Ср
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём получения информации идентификации/аутентификации, соответствующей учётной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условиях: – наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учётная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего, его отключили); – наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	2	0.6	Ср
УБИ.169	Угроза наличия механизмов разработчика	Угроза заключается в возможности перехвата управления программой за счёт использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации. Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство	10	0	0.5	ср

УБИ.170	Угроза неправомерного шифрования информации	Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов	Внешний нарушитель с низким потенциалом	Объект файловой системы	10	2	0.6	Ср
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств и др.), подключённых к сети Интернет, за счёт захвата управления такими устройствам путём несанкционированной установки на них: – вредоносного ПО типа Backdoor для обеспечения нарушителя возможностью удалённого доступа/управления дискредитируемым вычислительным устройством; – клиентского ПО для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа «отказ в обслуживании» и др.). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	10	2	0.6	Ср

УБИ.172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	2	0.6	Ср
УБИ.173	Угроза «спама» веб-сервера	Угроза заключается в возможности неправомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов. Данная угроза обусловлена уязвимостями механизмов фильтрации сообщений, поступающих из сети Интернет. Реализация данной угрозы возможна при условии наличия в дискредитируемом веб-сервере активированного функционала, реализующего различные почтовые сервера, службы доставки мгновенных сообщений, блоги, форумы, аукционы веб-магазинов, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	2	0.6	ср

УБИ.174	Угроза «фарминга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём скрытного перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; – средств создания и запуска поддельного сайта; – специальных программных средств типа «эксплойт», реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик	10	2	0.6	ср
УБИ.175	Угроза «фишинга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме. Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга». Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; – средств создания и запуска поддельного сайта; – сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик	10	0	0.5	ср

		ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)						
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации	Внешний нарушитель с низким потенциалом	Средство защиты информации	10	2	0.6	Ср

УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). Реализуемость данной угрозы зависит от требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью, а также разницей между этими требованиями и фактическим уровнем обнаружения и исправления ошибок	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	10	0	0.5	ср
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счёт использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях: – наличие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему и сокрытие (с использованием существующих архивов, атрибутов «скрытый» или «только для чтения» и др.); – наличие у нарушителя привилегий на запуск таких утилит	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	2	0.6	ср

УБИ.179	Угроза несанкционированной модификации защищаемой информации	Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём. Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы	10	2	0.6	Ср
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	10	2	0.6	Ср
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путём перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечёт их срок действия (обычно, не более 5 минут). Реализация данной угрозы возможна при выполнении следующих условий: наличие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия; успешное осуществление нарушителем перехвата трафика между системой и пользователем	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	10	0	0.5	ср

УБИ.182	Угроза физического устаревания аппаратных компонентов	Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем	Внутренний нарушитель с низким потенциалом	Аппаратное средство	10	5	0.75	Вы
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных. Данная угроза обусловлена наличием у автоматизированной системы управления технологическими процессами программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к: – блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия; – нарушению штатного хода технологических процессов; – частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя; – аварийной ситуации в критической системе информационной инфраструктуры.	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель со средним потенциалом	Программное обеспечение автоматизированной системы управления технологическими процессами	10	0	0.5	Ср

УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: – персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); – информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); – данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); – видеоданные, снимаемые видеокамерами мобильного устройства; – аудиоданные, снимаемые микрофоном устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	10	0	0.5	ср
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки средства защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к конфигурационным файлам средства защиты информации. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Средство защиты информации	10	2	0.6	Ср

УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов в сети Интернет	Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение	10	0	0.5	Ср
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования. Угроза обусловлена наличием у средств защиты информации программной среды управления и взаимодействия с пользователями системы. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации	10	2	0.6	Ср
УБИ.188	Угроза подмены программного обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети Интернет. Реализация данной угрозы возможна при скачивании программного обеспечения в сети Интернет	Внутренний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	10	2	0.6	ср

УБИ.189	Угроза маскирования действий вредоносного кода	Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации. Реализация данной угрозы возможна при условии использования в системе устаревших версий средств защиты информации	Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение	10	2	0.6	Ср
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: – неограниченном доступе пользователя в сеть Интернет; – наличии у нарушителя сведений о сайтах, посещаемых пользователем	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	10	2	0.6	Ср
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: – применении пользователем сторонних дистрибутивов; – отсутствии антивирусной проверки перед установкой дистрибутива	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	10	0	0.5	Ср
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	10	0	0.5	ср

УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная у гроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов. Реализация данной угрозы возможна: – при условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения; – при отсутствии или недостаточной реализации мер межсетевого экранирования	Внешний нарушитель со средним потенциалом	Информационные ресурсы, объекты файловой системы	10	0	0.5	Ср
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Угроза заключается в возможности снятия нарушителем предустановленных производителем ограничений на конфигурирование привилегированных функций мобильного устройства. Данная угроза обусловлена наличием уязвимостей в операционных системах мобильного устройства, позволяющих получить доступ к настройкам привилегированных функций. Реализация данной угрозы возможна при получении нарушителем доступа к мобильному устройству	Внешний нарушитель с высоким потенциалом	Мобильное устройство	10	0	0.5	ср
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Угроза заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему. Данная угроза обусловлена ошибками в процессорах (например, ошибками в процессоре Intel поколения Haswell), позволяющими за счет создания специальных приложений осуществлять обход механизмов защиты, встроенных в операционную систему (например, механизма ASLR). Реализация данной угрозы возможна при: – инициировании коллизии в таблице целевых буферов - с ее помощью можно узнать участки памяти, где находятся конкретные фрагменты кода; – создании приложения, использующего эти фрагменты кода для обхода механизма защиты; – запуске данного приложения в связке с эксплойтом какой-либо уязвимости самой операционной системы для создания возможности удаленного запуска вредоносного кода	Внешний нарушитель с высоким потенциалом	Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)	10	0	0.5	ср

УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем	Внешний нарушитель с высоким потенциалом	Мобильное устройство (аппаратное устройство)	10	0	0.5	ср
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Угроза заключается в возможности хищения с использованием вредоносной программы аутентификационной информации пользователей, их счетов, хранящейся во временных файлах cookie, и передачи этой информации нарушителям через открытый RDP-порт. Данная угроза обусловлена недостаточностью мер антивирусной защиты, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена непринятием мер по стиранию остаточной информации из временных файлов (очистке временных файлов). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	Внешний нарушитель со средним потенциалом	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	10	2	0.6	ср
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	Внешний нарушитель со средним потенциалом	Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)	10	2	0.6	Ср

УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Мобильное устройство и запущенные на нем приложения (программ-ное обеспечение, аппаратное устройство)	10	0	0.5	ср
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности хищения данных пользователя с его мобильного устройства через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающейся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Данные пользователя мобильного устройства (аппаратное устройство)	10	0	0.5	ср
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификацион ной информации в браузере	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации. Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации. Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации	Внешний нарушитель со средним потенциалом	Аутентифика ционные данные пользователя (программ-ное обеспечение)	10	0	0.5	ср

УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Угроза заключается в возможности установки приложений на виртуальные машины мобильных устройств, работающих под управлением операционной системы Android, несанкционированно запущенных внедренной вредоносной программой. Вредоносная программа запускает виртуальную машину на мобильном устройстве, размещает (устанавливает) в этой виртуальной машине неограниченное количество приложений. Данная угроза обусловлена недостаточностью мер по контролю за запуском прикладного программного обеспечения, что позволяет выполнить неконтролируемый запуск вредоносного прикладного программного обеспечения по факту совершения пользователем различных действий в системе (например, при попытке закрытия пользователем нежелательной рекламы). Реализация данной угрозы возможна при условии наличия на мобильном устройстве вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение	Внешний нарушитель со средним потенциалом	Мобильные устройства (аппаратное устройство, программное обеспечение)	10	0	0.5	ср
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Угроза заключается в возможности хищения данных с неподключенных к сети Интернет компьютеров за счет компрометации их аппаратных элементов или устройств коммутационного оборудования (например, маршрутизаторов), оснащенных LED-индикаторами, фиксации мерцания этих индикаторов и расшифровки полученных результатов. Реализация данной угрозы обусловлена тем, что существует возможность несанкционированного получения управления этими индикаторами (с помощью специальной прошивки или повышения привилегий и выполнения вредоносного кода), позволяющего передавать информацию путем ее преобразования в последовательность сигналов индикаторов компьютеров и коммутационного оборудования. Реализация данной угрозы возможна при условии, что злоумышленником получен физический доступ к компрометируемому компьютеру или коммутационному оборудованию для установки средства визуального съема сигналов LED-индикаторов	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Программное обеспечение	10	0	0.5	ср

УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах. Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации. Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет	Внешний нарушитель со средним потенциалом	Аппаратное устройство	10	2	0.6	Ср
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Угроза заключается в возможности нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов. Реализация данной угрозы обусловлена тем, что на компьютере установлено средство защиты информации, реализующее функцию блокирования файлов	Внешний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение	10	2	0.6	Ср
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Угроза заключается в прекращении работы оборудования с ЧПУ, вызванном изменением геолокационной информации о данном оборудовании. Угроза обусловлена геолокационной привязкой оборудования с ЧПУ к конкретной географической координате при пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации	Внешний нарушитель с высоким потенциалом	Аппаратное устройство	10	0	0.5	ср
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Угроза заключается в несанкционированном получении доступа к параметрам настройки информации в оборудовании с ЧПУ посредством использования специальных «мастер-кодов» (инженерных паролей), «жестко прописанных» (не изменяемых путем конфигурирования) в программном обеспечении данного оборудования. Угроза обусловлена необходимостью проведения ремонтных работ при сбоях в ПО оборудования с ЧПУ представителями производителя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение	10	0	0.5	ср
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной	Угроза заключается в возможности использования вычислительных ресурсов средств вычислительной техники для осуществления сторонних вычислительных процессов. Угроза реализуется за счет	Внешний нарушитель с низким потенциалом, Внешний нарушитель со средним	Средство вычислительной техники, мобильное устройство	10	2	0.6	ср

	техники	внедрения в средства вычислительной техники вредоносной программы, содержащей код, реализующий использования вычислительных ресурсов для своих нужд (в частности, для майнинга криптовалюты). Данная угроза обусловлена недостаточностью следующих мер защиты информации: – мер по антивирусной защите, что позволяет выполнить установку и запуск вредоносной программы; – мер по ограничению программной среды, что позволяют нарушителю осуществлять бесконтрольный запуск программных компонентов.	потенциалом, Внутренний нарушитель с низким потенциалом, Внутренний нарушитель со средним потенциалом					
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Угроза заключается в возможности получения доступа к защищенной памяти из программы, не обладающей соответствующими правами, в результате эксплуатации уязвимостей, позволяющих преодолеть механизм разграничения доступа, реализуемый центральным процессором. Реализация данной угрозы обусловлена наличием уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении инструкций процессора. Ошибка контроля доступа обусловлена следующими факторами: 1) отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти; 2) отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения; 3) хранение данных ядра операционной системы в адресном пространстве процесса. Реализация данной угрозы возможна из-за наличия процессоров, имеющих аппаратные уязвимости и отсутствия соответствующих обновлений	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное устройство	10	2	0.6	ср
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Угроза заключается в возможном нарушении функционирования программных, программно-аппаратных элементов информационной системы или информационной системы в целом из-за некорректной работы установленных обновлений (патчей) системного программного обеспечения. Угроза обусловлена наличием критических ошибок, дефектов, уязвимостей в используемом программном обеспечении информационной системы. Реализация данной угрозы возможна при условии установки обновлений на программно-аппаратные компоненты информационной системы	Внутренний нарушитель с высоким потенциалом	Аппаратное устройство, микропрограммное, системное и прикладное программное обеспечение	10	0	0.5	ср

УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Угроза заключается в возможности деструктивного воздействия на информационную систему и обрабатываемую ею информацию в результате работы программного обеспечения, используемого для администрирования информационных систем. Данная угроза связана со слабостями процедуры проверки пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования информационных систем. Реализация данной угрозы возможна в случае, если в информационной системе используется программное обеспечение администрирования информационных систем, которое в качестве исходных данных использует конфигурационные файлы, сформированные на основе пользовательских данных	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	10	2	0.6	Ср
УБИ.212	Угроза перехвата управления информационной системой	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам информационной системы в результате подмены средств централизованного управления информационной системой или её компонентами. Данная угроза обусловлена наличием у средств централизованного управления программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данным средствам централизованного управления, а также недостаточностью мер по разграничению доступа к ним. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия со средствами централизованного управления	Внутренний нарушитель со средним потенциалом	Инфраструк-тура информационных систем	10	2	0.6	Ср
УБИ.213	Угроза обхода многофакторной аутентификации	Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации. Данная угроза обусловлена: – наличием уязвимостей программного обеспечения; – слабостями мер антивирусной защиты и разграничения доступа. Реализация данной угрозы возможна: – в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников;	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя	10	0	0.5	ср

		– при наличии у него привилегий установки программного обеспечения						
Угрозы из Базовой модели угроз								
ТКУ 001	Угроза утечки акустической информации С ПРИМЕНЕНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ	Наличие функций голосового ввода или функции воспроизведения акустическими средствами	Внешний нарушитель с высоким потенциалом, внутренний нарушитель с высоким потенциалом	Рабочая станция	10	0	0.5	Ср
ТКУ 002								
ТКУ 003	Угроза несанкционированного съёма информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения	Перехват (просмотр) защищаемой информации может осуществляться посторонними лицами с расстояния прямой видимости из-за пределов контролируемой зоны с использованием оптических (оптикоэлектронных) средств	Внешний нарушитель с высоким потенциалом	Рабочая станция	10	0	0.5	Ср
ТКУ 004	Угроза утечки информации по каналам побочных электромагнитных излучений и наводок	Угроза заключается в возможности перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке защищаемой информации техническими средствами	Внешний нарушитель с высоким потенциалом	Сервер, рабочая станция, носитель информации	10	0	0.5	ср
ТКУ 005	Угроза внедрения программной, программно-аппаратной закладки на автоматизированное рабочее место	Угроза реализуется за счет внедрения (установки) в средства вычислительной техники программной или программно-аппаратной закладки, обеспечивающую съем и (или) передачу защищаемой информации, а также при определенных условиях несанкционированный доступ	Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом	Сервер, рабочая станция,	10	0	0.5	Ср
ТКУ 005	Угрозы выявления или подбора паролей	Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты	Внутренний нарушитель с низким потенциалом	Учётные данные пользователя	10	2	0.6	Ср
Иные источники угроз								
ИИУ 001	Угроза сбоя системы электроснабжения	Перебои в электроснабжении могут привести к сбоям в работе ИСПДн или средств вычислительной техники, что может вызвать к потери или несохранению информации, а также нарушению ее доступности в ИСПДн	Внутренний нарушитель с низким потенциалом	Сервер, рабочая станция	10	5	0.75	вы
ИИУ 002	Угроза использования не учтенных отчуждаемых носителей информации	Угроза заключается в возможности несанкционированного копирования защищаемой информации на съемные носители информации	Внутренний нарушитель с низким потенциалом	Носитель информации	10	5	0.75	Вы
ИИУ 003	Угроза вывода из строя	Угроза заключается в возможности умышленного/неумышленного	Внутренний нарушитель с	Сервер, рабочая	10	2	0.5	Ср

	автоматизированные рабочие места, сервера или каналы связи	выведения из строя внутренним нарушителем автоматизированные рабочие места, сервера или каналы связи, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к автоматизированным рабочим местам, серверам или каналам связи. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к автоматизированному рабочему месту, серверу или каналу связи.	низким потенциалом	станция, каналы связи				
ИИУ 004	Угроза несанкционированного отключения средств антивирусной защиты информации	Угроза заключается в возможности умышленного/неумышленного нарушения безопасности защищаемой информации пользователя, путем заражения вредоносными программами (вирусами) автоматизированного рабочего места. Реализация данной угрозы возможна при условии наличия у пользователя возможности отключения средства антивирусной защиты.	Внутренний нарушитель с низким потенциалом	Сервер, рабочая станция	10	2	0.6	Ср
ИИУ 005	Угроза утраты, кражи носителей информации содержащих ключи электронной подписи	Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы, доступных владельцу ключевого носителя в ИСПДн.	Внутренний нарушитель с низким потенциалом	Носитель информации	10	2	0.6	ср
ИИУ 006	Угроза неантропогенного (стихийного) характера, например удары молнии, пожары, наводнения и т.п.	Угроза заключается в возможности нарушения работоспособности ИСПДн, а также доступности и целостности защищаемой информации		Сервер, рабочая станция, носитель информации	10	5	0.75	вы